Claims

1. A method of authenticating the identity of a user to determine access to a system, comprising:

providing a plurality of factor-based data instances corresponding to a user;

evaluating the factor-based data instances to determine if the user's identity is authenticated;

restricting the user's access to the system if the user's identity is not authenticated; and

granting the user's access to the system if the user's identity is authenticated.

2. The method of claim 1, further comprising providing an authentication value, based on the evaluation determination.

3. The method of claim 1, wherein restricting the user's access includes denying the user's access.

4. The method of claim 1, wherein the factor-based data instances include a knowledge-based data instance.

5. The method of claim 1, wherein the factor-based data instances include a possession-based data instance.

6. The method of claim 1, wherein the factor-based data instances include a biometric-based data instance.

7. A method of authenticating the identity of a user to determine access to a system, comprising:

providing a plurality of factor-based data instances corresponding to a user, including at least one modified data instance based on a second data instance of the plurality of factor-based data instances;

generating a key based on a first data instance of the plurality of factor-based data instances;

applying the key to the at least one modified data instance to generate a recovered data instance;

interrogating the recovered data instance against the second data instance to generate an authentication value as a result of a correspondence evaluation;

restricting the user's access to the system based at least in part on an invalid authentication value; and

granting the user's access to the system based at least in part on a valid authentication value.

8. The method of claim 7, wherein the authentication value is a first authentication value, the method further comprising combining the first authentication value with at least one other authentication value, to generate a combined authentication value.

9. The method of claim 7, wherein restricting the user's access includes denying the user's access.

10. The method of claim 7, wherein the factor-based data instances include a knowledge-based data instance.

11. The method of claim 7, wherein the factor-based data instances include a possession-based data instance.

12. The method of claim 7, wherein the factor-based data instances include a biometric-based data instance.

13. A method of authenticating the identity of a user to determine access to a system, comprising:

providing a possession-based data instance, a modified version of the possession-based data instance, a knowledge-based data instance, a biometric-

based data instance, and a modified version of the biometric-based data instance;

generating a key based on the knowledge-based data instance;

applying the key to the modified version of the possession-based data instance to generate a first recovered data instance;

interrogating the first recovered data instance against the possession-based data instance to generate a possession value as a result of a first correspondence evaluation;

applying the key to the modified version of the biometric-based data instance to generate a second recovered data instance;

interrogating the second recovered data instance against the biometric-based data instance to generate a biometric value as a result of a second correspondence evaluation;

combining the key, the possession value, and the biometric value to form an authentication value;

restricting the user's access to the system if the user's identity is not authenticated, based at least in part on the authentication value; and

granting the user's access to the system if the user's identity is authenticated, based at least in part on the authentication value.

14. The method of claim 13, wherein restricting the user's access includes denying the user's access.

15. The method of claim 13, wherein the modified version of the biometric-based data instance is a first modified version of the biometric-based data instance, and the biometric value is a second modified version of the biometric-based data instance.

16. The method of claim 15, wherein the biometric value is a cryptographic hash of the biometric-based data instance.

17. The method of claim 13, wherein restricting the user's access to the system and granting the user's access to the system is based on a modified version of the authentication value.

18. The method of claim 17, wherein the modified version of the authentication value is a cryptographic hash of the authentication value.

19. A method of authenticating the identity of a user to determine access to a system, comprising:

providing a possession-based data instance, a stored biometric-based data instance, and a read biometric-based data instance;

interrogating the stored biometric-based data instance against the read biometric-based data instance to generate a biometric value as a result of a correspondence evaluation;

combining the possession-based data instance and the biometric value to form an authentication value;

evaluating the authentication value to determine if the user's identity is authenticated;

restricting the user's access to the system if the user's identity is not authenticated, based at least in part on the authentication value; and

granting the user's access to the system if the user's identity is authenticated, based at least in part on the authentication value.

20. The method of claim 19, wherein restricting the user's access includes denying the user's access.

21. The method of claim 19, wherein the biometric value is a modified version of the biometric-based data instance.

22. The method of claim 21, wherein the biometric value is a cryptographic hash of the biometric-based data instance.

23. The method of claim 19, wherein restricting the user's access to the system and granting the user's access to the system is based on a modified version of the authentication value.

24. The method of claim 23, wherein the modified version of the authentication value is a cryptographic hash of the authentication value.

25. A method of authenticating the identity of a user to determine access to a system, comprising:

providing a possession-based data instance, a biometric-based data instance, and a modified version of the biometric-based data instance;

applying the possession-based data instance to the modified version of the biometric-based data instance to generate a recovered data instance;

interrogating the recovered data instance against the biometric-based data instance to generate a biometric value as a result of a correspondence evaluation;

combining the possession-based data instance and the biometric value to form an authentication value;

evaluating the authentication value to determine if the user's identity is authenticated;

restricting the user's access to the system if the user's identity is not authenticated, based at least in part on the authentication value; and

granting the user's access to the system if the user's identity is authenticated, based at least in part on the authentication value.

26. The method of claim 25, wherein restricting the user's access includes denying the user's access.

27. The method of claim 25, wherein the modified version of the biometric-based data instance is a first modified version of the biometric-based data instance, and the biometric value is a second modified version of the biometric-based data instance.

28. The method of claim 27, wherein the biometric value is a cryptographic hash of the biometric-based data instance.

29. The method of claim 25, wherein restricting the user's access to the system and granting the user's access to the system is based on a modified version of the authentication value.

30. The method of claim 29, wherein the modified version of the authentication value is a cryptographic hash of the authentication value.

31. In a multi-level access system, a method of securing an object at a multiple-level access level, comprising:

receiving, from a user, a profile key encryption key corresponding to the multiple-level access level;

selecting an object to secure;

selecting a profile associated with the user, wherein the profile includes

a domain value,

an encrypted profile encryption key, and

a credential, wherein the credential includes

an encrypted credential public key,

an encrypted credential public key encryption key, and

a multiple-level access identifier;

selecting the credential based on a comparison of the multiple-level access level and the multiple-level access identifier;

generating a working key, including

generating a random value, and

binding at least the domain value and the random value together to form the working key;

encrypting the object with the working key;

generating a random value encryption key, including

decrypting the encrypted credential public key encryption key with at least the profile key encryption key,

decrypting the encrypted credential public key with at least the decrypted credential public key encryption key,

generating an ephemeral key pair including an ephemeral private key and an ephemeral public key,

generating a shared value based on at least the ephemeral private key and the decrypted credential public key, and

generating the random value encryption key based on at least the shared value;

encrypting the random value with at least the random value encryption key; and

providing the encrypted object, the ephemeral public key, and the encrypted random value for an authorized recipient.

32. The method of claim 31, wherein

the profile further includes a profile initialization vector, and

decrypting the encrypted credential public key encryption key includes decrypting the encrypted credential public key encryption key with the profile key encryption key and the profile initialization vector.

33. The method of claim 32, wherein

the credential further includes a credential initialization vector, and

decrypting the encrypted credential public key includes decrypting the encrypted credential public key with the decrypted credential public key encryption key and the credential initialization vector.

34. The method of claim 33, wherein the multiple-level access level corresponds to the multiple-level access identifier.

35. The method of claim 33, wherein the multiple-level access level is identical to the multiple-level access identifier.

36. The method of claim 33, wherein the multiple-level access level is lower than the multiple-level access identifier.

37. The method of claim 33, wherein the multiple-level access level is higher than the multiple-level access identifier.

38. In a computer system comprising a token communicatively connected to a provider, a method of authenticating a user to use a system, comprising:

generating, by the token, a random value;

sending, by the token, the random value, a token ID, and a salt value to the provider;

providing, by the user, a user password to the provider;

generating, by the provider, a derived key based at least in part on the salt value and the password;

applying, by the provider, a first key-based hash algorithm, using the derived key, to the token ID to provide a first hash value;

generating, by the provider, a first challenge data instance based at least in part on the random value and the first hash value;

sending, by the provider, the first challenge data instance to the token;

generating, by the provider, a token unlock key based at least in part on the derived key;

sending, by the provider, the token unlock key to the token;

generating, by the token, a second challenge data instance based at least in part on the random value and a second hash value, wherein the second hash value is stored on the token and is based on the token ID;

determining, by the token, whether the first and second challenge data instances match;

terminating, by the token, the method, if the first and second challenge data instances are determined not to match; and

if the first and second challenge data instances are determined to match, then

establishing an encrypted data transfer system between the token and the provider,

unlocking with the token unlock key, by the token, locked first private data stored on the token, and

authenticating the user for secured use of the system based at least in part on the unlocked first private data.

39. The method of claim 38, wherein the derived key is generated with a password-based encryption algorithm.

40. The method of claim 39, wherein the password-based encryption algorithm is based at least in part on PKCS #5.

41. The method of claim 38, wherein the first hash algorithm is a hash function-based message authentication code.

42. The method of claim 38, wherein generating the token unlock key includes hashing the derived key to provide the token unlock key.

43. The method of claim 38, wherein generating the first challenge data instance includes mathematically binding together the first hash value and the random value to provide the first challenge data instance.

44. The method of claim 38, wherein

generating the first challenge data instance comprises mathematically binding together the first hash value and the random value to provide the first challenge data instance; and

generating the second challenge data instance comprises mathematically binding together the second hash value and the random value to provide the second challenge data instance.

45. The method of claim 38, wherein

generating the first challenge data instance comprises mathematically binding together the first hash value and the random value to provide a first resulting value, and hashing the first resulting value to provide the first challenge data instance; and

generating the second challenge data instance comprises mathematically binding together the second hash value and the random value to provide a second resulting value, and hashing the second resulting value to provide the second challenge data instance.

46. The method of claim 38, wherein establishing the encrypted data transfer system comprises generating, by at least one of the token and the provider, a shared key.

47. The method of claim 46, wherein the shared key is a shared session key.

48. The method of claim 46, wherein the shared key is generated based at least in part on shared data that includes a Diffie-Hellman parameter set.

49. The method of claim 38, further comprising:

combining, by the provider, a message and a present message value to provide a modified message;

encrypting, by the provider, the modified message, using a shared key, to provide an encrypted message;

combining, by the provider, the modified message and the random value to provide a first pre-hash value;

applying, by the provider, the first key-based hash algorithm, using the first hash value, to the first pre-hash value to provide a third hash value;

combining, by the provider, the encrypted message and the third hash value to provide a signed message;

sending, by the provider, the signed message to the token;

extracting, by the token, the encrypted message and the third hash value from the signed message received from the provider;

decrypting, by the token, the encrypted message, using the shared key to provide the modified message;

extracting, by the token, the message and the present message value from the decrypted encrypted message;

combining, by the token, the message, the present message value, and the random value to provide a second pre-hash value;

applying, by the token, the first key-based hash algorithm, using the second hash value, to the second pre-hash value to provide a signing hash value; and

validating, by the token, the message, if the signing hash value and the third hash value match and the present message value is greater than a prior message value stored on the token.

50. The method of claim 38, further comprising

combining, by the token, a message and a present message value to provide a modified message;

encrypting, by the token, the modified message, using a shared key, to provide an encrypted message;

combining, by the token, the modified message and the random value to provide a first pre-hash value;

applying, by the token, the first key-based hash algorithm, using the second hash value, to the first pre-hash value to provide a third hash value;

combining, by the token, the encrypted message and the third hash value to provide a signed message;

sending, by the token, the signed message to the provider;

extracting, by the provider, the encrypted message and the third hash value from the signed message received from the token;

decrypting, by the provider, the encrypted message, using the shared key to provide the modified message;

extracting, by the provider, the message and the present message value from the decrypted encrypted message;

combining, by the provider, the message, the present message value, and the random value to provide a second pre-hash value;

applying, by the provider, the first key-based hash algorithm, using the first hash value, to the second pre-hash value to provide a signing hash value; and

validating, by the provider, the message, if the signing hash value and the third hash value match and the present message value is greater than a prior message value stored on the provider.

51. The method of claim 38, wherein unlocking the locked first private data comprises decrypting the locked first private data with the token unlock key.

52. The method of claim 38,

wherein the unlocked first private data includes at least one user credential associated with the user; and

wherein authenticating the user includes providing at least one of the at least one user credential to the system to grant the user cryptographic reading authority.

53. The method of claim 38,

wherein the unlocked private data includes at least one user credential associated with the user, and

wherein authenticating the user includes providing at least one of the at least one user credential to the system to grant the user cryptographic writing authority.

54. The method of claim 38, wherein the system further comprises a biometric reader communicatively connected to the provider, the locked first private data includes an encrypted biometric template, and the method further comprises:

sending, by the token, the encrypted biometric template to the provider;

decrypting, by the provider, the encrypted biometric template with the derived key;

providing, by the user, a biometric sample via the biometric reader to the provider;

determining, by the token, whether the biometric sample corresponds to the decrypted biometric template;

terminating the method, by the provider, if the biometric sample is determined not to correspond to the decrypted biometric template;

if the biometric sample is determined to correspond to the decrypted biometric template,

applying, by the provider, one of the first key-based algorithm and a second key-based algorithm, using the derived key, to the decrypted biometric template to provide a third hash value,

generating, by the provider, a third challenge data instance based at least in part on the third hash value and the random value, and

sending, by the provider, the third challenge data instance to the token;

generating, by the token, a fourth challenge data instance based at least in part on the random value and a fourth hash value, wherein the fourth hash value is stored on the token and is based on the biometric template;

determining, by the token, whether the third and fourth challenge data instances match;

terminating, by the token, the method if the third and fourth challenge data instances are determined not to match; and

if the third and fourth challenge data instances are determined to match, unlocking with at least a portion of the unlocked first private data, by the token, locked second private data stored on the token;

wherein authenticating the user for secured use of the system further requires that the third and fourth data instances are determined to match.

55. The method of claim 38, wherein the system further comprises a biometric reader communicatively connected to the token, the locked first private data includes an encrypted biometric template, and the method further comprises:

providing, by the user, a biometric sample via the biometric reader to the token;

decrypting, by the token, the encrypted biometric template with the derived key;

determining, by the token, whether the biometric sample corresponds to the decrypted biometric template;

terminating the method, by the token, if the biometric sample is determined not to correspond to the decrypted biometric template; and

if the biometric sample is determined to correspond to the decrypted biometric template, unlocking, by the token, with at least a portion of the unlocked first private data, locked second private data stored on the token;

wherein authenticating the user for secured use of the system further requires that the biometric sample is determined to correspond to the decrypted biometric template.

56. The method of claim 55, wherein the biometric reader is integral with the token.

57. The method of claim 38, wherein establishing the encrypted data transfer system comprises encrypting messages exchanged between the token and the provider with an encryption key.

58. The method of claim 57, further comprising:

sending, by the token, an encrypted instance of the encryption key and an encrypted user profile associated with the user to the provider;

applying, by the provider, a key derivation function to the derived key and the first hash value to provide a cryptographic key;

decrypting, by the provider, the encrypted instance of the encryption key;

decrypting, by the provider, the encrypted profile with the encryption key; and

providing, by the provider, the decrypted user credential to the system to grant the user at least one of cryptographic reading authority and cryptographic writing authority.

59. In a computer system comprising a token communicatively connected to a provider, a method of authenticating a user to use a system, comprising:

sending, by the token, a token ID, a salt value, an encrypted encryption key, and an encrypted user profile to the provider;

providing, by the user, a user password to the provider;

generating, by the provider, a derived key based at least in part on the salt value and the password;

applying, by the provider, a first key-based hash algorithm, using the derived key, to the token ID to provide a first hash value;

applying, by the provider, a key derivation function to the derived key and the first hash value to provide a cryptographic key;

decrypting, by the provider, the encrypted instance of the encryption key;

decrypting, by the provider, the encrypted profile with the encryption key; and

providing, by the provider, the decrypted user credential to the system to grant the user at least one of cryptographic reading authority and cryptographic writing authority.